the trust level of the environment in which the encryptor is located. The encryptor encrypts this symmetric key for one or more intended recipients using an asymmetric technique commensurate with a high-trust environment. In the case of the encryptor residing in the low-trust environment, the encryptor additionally encrypts this symmetric key using an asymmetric encryption public key of the originator itself (or alternatively, that of a third party). Decryption equipment in all environments uses the decryption process corresponding to an algorithm identifier included by the originator. In all cases, the asymmetric encryption/decryption process used for each specific recipient is of a strength commensurate with the trust level of that recipient's own environment. (Van Oorschot, Abstract)

Applicants submit that Van Oorschot fails to disclose "encrypting the first key with a second key", as recited in claim 16. Specifically, Applicants' independent claim 16 reads as follows:

16. A method of updating a cryptographic key used for decrypting distributed data, the method comprising:
generating a first key for decrypting the distributed data, the first key of a first length;
encrypting the first key with a second key, the second key of a second length, wherein the second length is longer than the first length; and
distributing the encrypted first key. (emphasis added)

The present invention uses multiple public/private key pairs of varying levels of security. The lower-security level includes keys which are small in length, which are changed relatively often, and which require low resources to implement their coding functions. When it is desired to change key pairs of low security, a key pair at a higher security level (i.e., longer length keys) than the lower-security level keys is used to transfer the new lower-security public keys to devices using the higher-security keys.

The higher security keys can, in turn, be changed at a frequency lower than the lower-security keys. The higher-security keys require a higher level of resources to perform their coding operations. This approach of using keys of escalating levels of security to replace lower-security keys, where the higher-security keys require more resources, are more secure, and are replaced less often than the lower-security keys, can be followed as many times as is desired to create a hierarchy of public key uses with the result that the lower-security operations can be performed quickly while the overall system security is high.

In contrast, Van Oorschot fails to teach updating a cryptographic key used for decrypting distributed data. (See Van Oorschot) In Van Oorschot, a symmetric key is generated to encrypt a message. (See Van Oorschot, Fig. 1) The symmetric key is then encrypted with the public key of the sender and separately encrypted with the public key of the receiver. (See Van Oorschot, Fig. 1) The encrypted versions of the symmetric key are then transmitted with the encrypted message. (See Van Oorschot, Fig. 1) Upon receipt of the message by the recipient, the header of the message is decrypted to produce the symmetric key and the symmetric key is used to decrypt the message. (See Van Oorschot, Fig. 2) Oorschot fails to teach the present invention as claimed since the symmetric key that is transmitted is used **only** to decrypt the message with which the symmetric key is transmitted and **not** to update a previous symmetric key. Van Oorschot is completely devoid of the disclosure of encrypting a replacement key with a second key in the manner recited by Applicants' claims.

Therefore, Applicants submit that independent claim 16 is patentable over Van Oorschot. Claims 17-19 are patentable at least by virtue of depending from their respective base claim. Applicants respectfully request withdrawal of the rejection.

**II. Rejection under 35 U.S.C. § 103(a)**

Claims 1-7 and 10-15 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Menezes et al. (Handbook of Applied Cryptography, 1997, section 13.3.1, pps. 551-553) (Menezes) in view of Weiant, Jr. et al. (U.S. Patent No. 6,044,350, issued March 28, 2000) (Weiant). Applicant respectfully disagrees.

Applicants submit that Menezes in view of Weiant fails to disclose that "the second key is used in cryptographic processing operations for the first key at a second rate that is less often than the first rate and that requires a second cryptographic processing time greater than the first cryptographic processing time" as recited in Applicants' independent claim 1. Applicants also submit that Menezes in view of Weiant fails to disclose that "the second asymmetrical cryptographically processed key is used in an asymmetric cryptographic processing operation at a second level of complexity requiring a second amount of resources by the processing device that is higher than the first amount of resources" as recited in Applicants' independent claim 10.

The Examiner conceded that Menezes fails to disclose that "the second key requires a second cryptographic processing time greater than the first cryptographic processing time". In order to cure the Examiner's perceived deficiency of Menezes, Weiant is cited.

Weiant **only** discloses the general proposition that different keys may have different associated processing times. (See Weiant, Fig. 3) However, Weiant, like

Menezes fails to disclose that "the second key…**requires** a second cryptographic processing time greater than the first cryptographic processing time", as recited in claim 1 or "the second asymmetrical cryptographically processed key is used in an asymmetric cryptographic processing operation at a second level of complexity **requiring** a second amount of resources by the processing device that is higher than the first amount of resources", as recited in claim 10.

The cited portion of Menezes does not discuss methods of performing key replacements. Therefore, the cited portion of Menezes also says nothing about the length, complexity, time to process, resources to process, etc. of the replacement key relative to that of the key used to process the replacement key. Therefore, at least for the above reasons, there would be no motivation to combine Menezes with Weiant to arrive at the present invention as claimed.

In view of the above arguments, Applicants submit that independent claims 1 and 10 are patentable over Menezes in view of Weiant. Claims 2-7 and 11-15 are patentable at least by virtue of depending from their respective base claim. Applicants respectfully request withdrawal of the rejection.

Date: July 12, 2007

Respectfully submitted,

By: /Thomas Bethea, Jr./
Thomas Bethea, Jr.
Reg. No.: 53,987

Motorola Connected Home Solutions
101 Tournament Drive
Horsham, PA 19044
(215) 323-1850